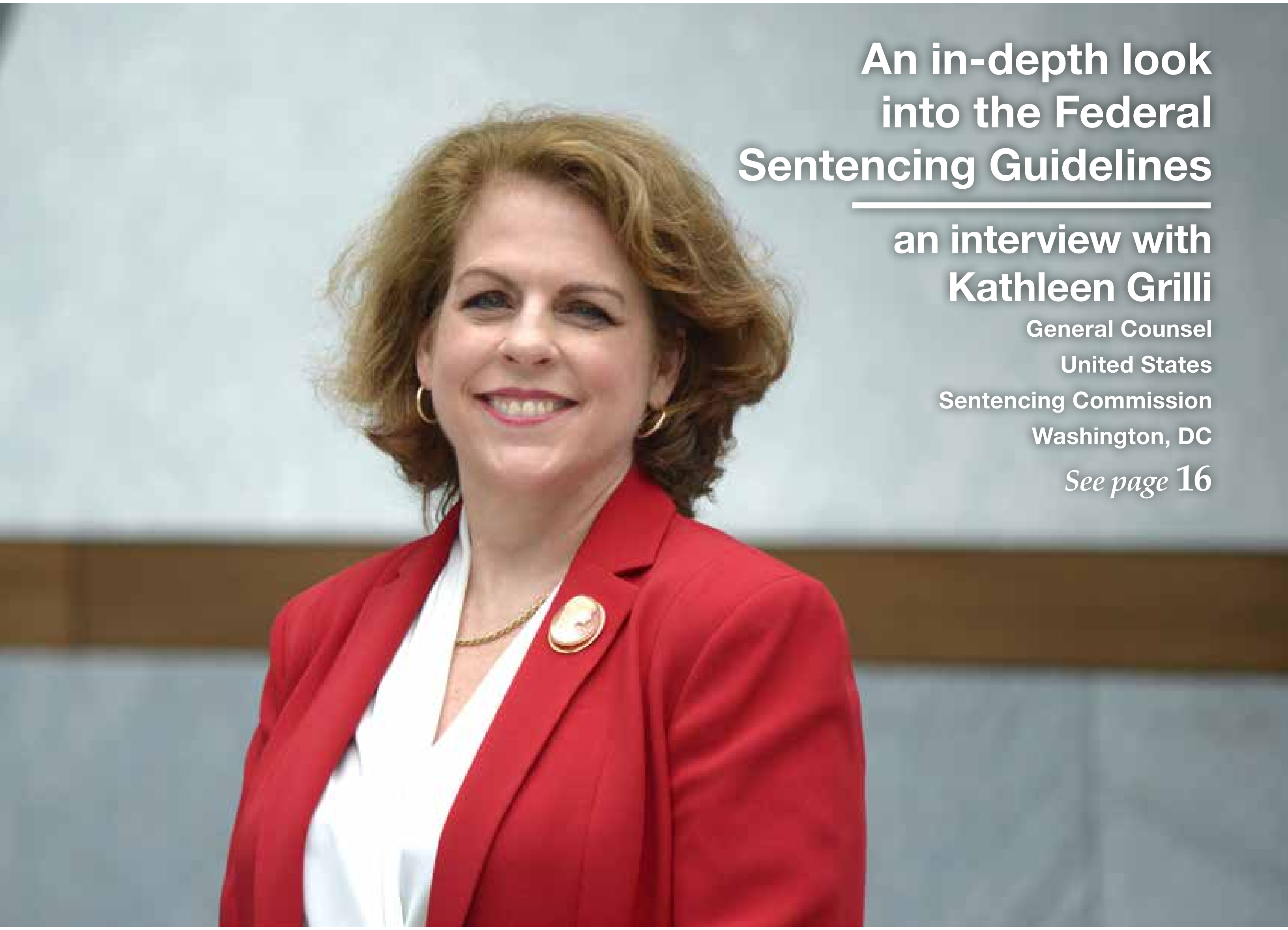
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

September 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



An in-depth look into the Federal Sentencing Guidelines

an interview with Kathleen Grilli
General Counsel
United States
Sentencing Commission
Washington, DC

See page 16

> “Every year, fraud is one of the two top types of offenses for which organizations are sentenced...”
>
> *See page* 21

ARTICLES

Compliance
TODAY

EXECUTIVE EDITOR: Roy Snell, CHC, CCEP-F, CEO, HCCA
roy.snell@corporatecompliance.org

NEWS AND STORY EDITOR/ADVERTISING: Margaret R. Dragon
781-593-4924, margaret.dragon@corporatecompliance.org

COPY EDITOR: Patricia Mees, CHC, CCEP, 888-580-8373
patricia.mees@corporatecompliance.org

DESIGN & LAYOUT: Pete Swanson, 888-580-8373
pete.swanson@corporatecompliance.org

PROOFREADER: Bill Anholzer, 888-580-8373
bill.anholzer@corporatecompliance.org

PHOTOS ON FRONT COVER & PAGE 16: Steve O'Toole

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to *Compliance Today*, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

For Advertising rates, call Margaret Dragon at 781-593-4924. Send press releases to M. Dragon, 41 Valley Rd, Nahant, MA 01908.

Opinions expressed are not those of this publication or HCCA. Mention of products and services does not constitute endorsement. Neither HCCA nor CT is engaged in rendering legal or other professional services. If such assistance is needed, readers should consult professional counsel or other professional advisors for specific legal or ethical questions.

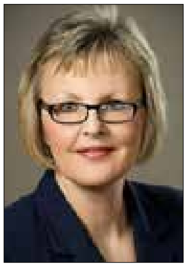
VOLUME 19, ISSUE 9

by Debbie Kiehl, FACMPE, CRCR

Credit card on file program

- » Due to increasing out-of-pocket expenses for patients, healthcare entities are exploring a "credit card on file" option to make patient payments more timely and efficient.
- » Credit card on file programs should use a certified PCI-DSS vendor to ensure the healthcare entity meets the credit card data security standard.
- » Develop policies and procedures for practice staff to follow, including a financial policy for the patients to review, and require patients to provide signed authorization for payments.
- » Penalties for non-compliance and/or a breach are maintained by the industry PCI Standards Council (can range from $2,000-$100,000 per month).
- » Penalties are levied on banks and credit card institutions and can be filtered down to the healthcare practice if credit card data is compromised.

Debbie Kiehl *(dkiehl@cokergroup.com) is a Senior Manager with Coker Group in Alpharetta, GA.* *bit.ly/in-DebbieKiehl*


Kiehl

With rising premiums and the popularity of employer-sponsored health savings accounts (HSAs), patients are facing higher out-of-pocket costs that could threaten their access to care. Increasingly, medical practices and hospitals are searching for methods to make it easier for patients to pay their out-of-pocket healthcare obligations. This has resulted in many healthcare entities implementing credit card on file (CCOF) processes to increase their revenue/cash by making it easier for patients to pay their out-of-pocket costs (e.g., copayments, co-insurance, deductibles, recurring payments).

A CCOF program provides a secure format to maintain the patient credit card information and affords the provider permission (from the patient) to charge the card on file after an insurance payer has processed and paid the claim. The remaining balance can then be processed for payment via secure format with the patient's credit card information.

This article reviews the necessary compliance steps a medical practice needs to take to ensure that credit card processing is secure and patients' credit card information is protected.

Secure transactions

Healthcare providers and practices must comply with the industry standards used by companies that process payments with credit, debit, or cash cards.

Payment Card Industry Data Security Standard-certified vendor

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security rules designed to ensure all businesses that accept, process, store, or transmit credit information remain in a secure environment. CCOF processing should be set up with a PCI DSS-certified vendor and adhere to the set of policies and procedures developed to protect credit, debit, and cash card transactions and prevent the misuse of cardholders' personal information. PCI DSS compliance is required by all card brands.[1] Using a third-party vendor will not preclude a business from being PCI-DSS certified.

Using a credit card processor that is PCI-DSS compliant

Most credit cards on file are used for recurring payments and/or where patients use their credit card frequently to pay for their healthcare services. In these instances, a PCI-DSS vendor offers card vaults. A payment vault and "tokenization" solution are the core of the PCI solution and assist e-commerce. The payment vault is a secure location used to store all patient credit card numbers. Once the credit card numbers have been inserted into the PCI vault, the practice receives a token that can be used in the future. The token can then be stored freely on the practice servers, because there is no way to decrypt the PCI token to determine the original credit card number.

> The practice should develop a policy and procedure algorithm for processing payments through a consent form mechanism.

Payment vault and tokenization

A payment vault is a secure location to protect the patient's credit card information. Once the credit card number has been inserted into the hosted PCI vault, the practice will receive a token that can be used in the future.[2] The token is a process where a primary account number is replaced with a surrogate value called a token.

Consent form

The practice should develop a policy and procedure algorithm for processing payments through a consent form mechanism. Once the CCOF is set-up with a secure PCI-DSS processor, the practice should ensure all their internal processes are in place. The practice should develop a policy and procedure for how the CCOF payments will be processed.

The practice should also draft and approve a consent form that the patient will sign prior to their first payment being processed and a policy on how the consent form will be provided to the patient. The practice must obtain patients' consent to process the charges on their credit or debit cards under the Electronic Funds Transfer Act (EFTA); otherwise it could be an unauthorized purchase.[3]

Policy and procedure

As part of the practice's compliance program, the practice should develop a financial policy and procedure that outlines the process for securing the patient's credit card information. Further, the practice should conduct regular training on this policy to ensure compliance with any federal, state, or local regulations.

The policy should outline the procedures for the practice employees' appropriate handling of credit and debit card transactions. The policy should also prohibit the practice staff from maintaining information on the cardholder in the practice.

Penalties for non-compliance and breach consequences

The PCI compliance is maintained by the industry standards body called PCI Security Standards Council (SSC). The standards are reinforced by five payment card brands: Visa, MasterCard, American Express, JCB International, and Discover. Each brand has their standards for monitoring.[4] The penalty for non-compliance with the PCI standards can range from $2,000-$100,000 per month. These violations are levied against banks and credit card institutions and can be filtered down to the healthcare practice if the cardholder data is compromised.[5]

Breach consequences

The consequences of a breach can be severe and can result in large financial penalties for the practice. Even if a company is 100% PCI compliant and validated, a breach in cardholder data may still occur. Cardholder breaches can result in the following losses for a merchant:

- $50-$90 fine per cardholder data compromised;
- Suspension of credit card acceptance by a merchant's credit card account provider;
- Loss of reputation with customers, suppliers, and partners;
- Possible civil litigation from breached customers; and
- Loss of customer trust, which may affect future sales.[6]

Conclusion

Because medical practices are seeing patients bearing a larger proportion of their healthcare costs, practices are forced to look for ways to improve their cash flow. However, to remain in compliance with regulations, it is important for the practice to ensure that the patient's credit card data is not compromised and is maintained in a secure format. The process will be successful through the correct set up with a PCI merchant and by complying with the practice policies and procedures.

[1] PCI ComplianceGruide.org: Welcome to the PCI Compliance Guide, frequently asked questions, #5. Available at http://bit.ly/2utZgrZ
[2] HostedPCI: Payment Vault and Tokenization. Available at http://bit.ly/2v0ZKsy
[3] Board of Governors of the Federal Reserve System, Regulation E: Electronic Fund Transfer Act. Available at http://bit.ly/2eJ1lMV
[4] PCI Security Standards Council: Organizational Structure. Available at http://bit.ly/2uRtqYN
[5] SecureWorks, http://bit.ly/2v18ONX
[6] Focus on PCI, PCI Noncompliant Consequences. Available at http://bit.ly/2vCqFYH